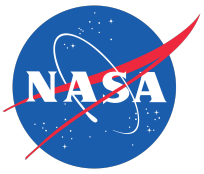

NASA TECHNICAL STANDARD

National Aeronautics and Space Administration

NASA-STD-2603
Approved: 2019-10-09

MINIMUM SECURITY AND PRIVACY REQUIREMENTS FOR AGENCY AND CENTER INFORMATION SYSTEM IMPLEMENTATIONS

v1.0 - 2019-10-09

TABLE OF CONTENTS

DOCUMENT HISTORY LOG

Status	Document Revision	Change Number	Approval Date	Description
Baseline	1.0		2019-10-09	Baseline Release

FOREWORD

This NASA Technical Standard and its companion Specification, NASA-SPEC-2603, *Minimum Security and Privacy Requirements for Agency and Center Information System Implementations*, are approved for use by NASA Headquarters and all NASA Centers. They are intended to provide common guidance for consistent application of information technology security requirements across NASA programs and projects.

Adherence to this Standard ensures compliance with Agency and Federal information technology security policies, mandates, and standards for enterprise technology system implementation.

Requests for information, corrections, or additions to this Standard should be directed to the NASA John H. Glenn Research Center at Lewis Field (GRC), Cybersecurity Standards and Engineering Team (CSET), MS 142-5, Cleveland, OH, 44135 or to standards-comments@lists.nasa.gov.

Michael Witt

Digitally signed by Michael Witt
Date: 2019.10.09 16:11:40
-04'00'

Michael Witt
Senior Agency Information Security Officer

1. SCOPE

1.1. Purpose

This NASA Technical Standard and its companion Specification, NASA-SPEC-2603, *Minimum Security and Privacy Requirements for Agency and Center Information System Implementations*, define information technology security and privacy requirements that must be considered for Agency implementations.

1.2. Applicability

This NASA Standard (STD) is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. This language applies to the Jet Propulsion Laboratory, a Federally Funded Research and Development Center, other contractors, grant recipients, or parties to agreements only to the extent specified or referenced in the appropriate contracts, grants, or agreements.

This NASA Standard (STD) applies to all NASA information technology (IT) and information resources, including operational technology, as defined by U.S. Federal Code 40 U.S.C. 11101. IT and information resources are defined as any equipment or system that is used in the acquisition, storage, retrieval, manipulation and/or transmission of data or information. Information resources include but are not limited to: computers, ancillary and peripheral equipment, software, firmware, and physical devices. This definition applies unless expressly excluded by the NASA Chief Information Officer (CIO).

All information systems developed, used, or operated by NASA, by a contractor of an executive agency, or by another organization on behalf of an executive agency shall apply this Standard and NASA-SPEC-2603. This Standard and NASA-SPEC-2603 shall apply to all information systems in all phases of life cycle, regardless of planned online or offline operating posture.

NPR 2810.1x, Security of Information Technology, clearly defines the role and responsibilities of information system owners (ISO) in relation to Agency information systems. These responsibilities include:

- Acquiring, developing, integrating, operating, modifying, and maintaining information systems.
- Ensuring system-level implementation of all Agency and Center requirements.
- Taking appropriate actions to identify and minimize or eliminate information system security deficiencies and weaknesses.

Standard and Specification guidance will be added, replaced, or removed as appropriate to align these responsibilities with Agency information security- and privacy-related program and project requirements.

1.3. Authority

The Agency Chief Information Officer (CIO) and Senior Agency Information Security Officer (SAISO) have authorized the Cybersecurity Standards and Engineering Team (CSET) via the Agency Security Configuration Standards (ASCS) initiative to create binding Technical Standards related to Agency cybersecurity topics.

The NASA Technical Standards Program (NTSP), sponsored by the Office of the NASA Chief Engineer, recognizes CSET as a standards-developing organization within the Agency. NTSP provides access to all technical standards at:

https://standards.nasa.gov/

The guidance in this Standard aligns with the Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 11, 2017).

“Shall” and “must” statements in this document impose an obligation to act. “Shall not” statements generally prohibit an action. “Should” statements imply an obligation to act, but not a necessity.

1.4. Tailoring

Tailoring of this NASA Technical Standard for application to a specific program, project, or system shall be formally documented as part of program or project requirements and approved by the responsible ISO and Authorizing Official (AO).

2. APPLICABLE DOCUMENTS

2.1. General

The documents listed in this section contain provisions that constitute requirements of this NASA Technical Standard as cited in the text.

The latest issuances of cited documents shall apply unless specific versions are designated.

Non-use of specifically designated versions shall be approved by the responsible Technical Authority.

The applicable documents are accessible at https://nodis3.gsfc.nasa.gov/ and https://standards.nasa.gov or may be obtained directly from the Standards Developing Body or other document distributors.

2.2. Government Documents

Document Number	Document Title
NPR 2810.x	*Security of Information Technology*
NASA-SPEC-2603	*Minimum Security and Privacy Requirements for Agency and Center Information System Implementations*
NASA-STD-2601	*Minimum Cybersecurity Requirements for Computing Systems*

2.3. Order of Precedence

This NASA Technical Standard establishes information technology security and privacy requirements that must be considered for Agency technology implementations, but does not supersede nor waive established Agency requirements found in other documentation.

3. ACRONYMS AND DEFINITIONS

Table 1. Acronyms and Abbreviations

AO	Authorizing Official
ASCS	Agency Security Configuration Standards
CIO	Chief Information Officer
CSET	Cybersecurity Standards and Engineering Team
ISO	Information System Owner
IT	Information Technology
NPR	NASA Procedural Requirement
NTSP	NASA Technical Standards Panel
OCIO	Office of the Chief Information Officer
RBD	Risk-Based Decision
RISCS	Risk Information and Security Compliance System
SAISO	Senior Agency Information Security Officer
STD	Standard

Definitions

Definitions regarding information technology security and related roles may be found in NPR 2810.1x.

4. OVERVIEW OF IT SECURITY AND PRIVACY REQUIREMENTS FOR AGENCY TECHNOLOGY PROGRAMS AND PROJECTS

4.1. Baseline IT Security Requirements for Agency Technology Projects

The NASA Office of the Chief Information Officer (OCIO) developed NASA-SPEC-2603 to provide a consistent set of cybersecurity guidelines that must be considered by all NASA projects. The baseline security requirements shall be evaluated and addressed as part of project planning, design, and testing. These baseline requirements should not be considered a complete list of cybersecurity requirements, as individual projects will likely still require some specific tailored security requirements. A cybersecurity engineer should be identified for all projects that will assist in both the baseline requirements and the development of the tailored security requirements necessary for the project.

4.1.1. Mandatory Baseline IT Security Requirements for Agency Technology Projects

The requirements outlined in NASA-SPEC-2603 shall be addressed by the project, and risk acceptance shall not be an option, unless indicated otherwise for individual requirements.

4.1.2. Risk-Based Decision (RBD) Eligible Baseline IT Security Requirements for Agency Technology Projects

All other technical requirements may not be fully implemented by the system and could be considered for risk acceptance. RBDs shall be requested via the Risk Information and Security Compliance System (https://riscs.nasa.gov, or RISCS). Rejection or approval by the AO that has been identified for the project must also be documented in RISCS. For each requirement that is risk-accepted, the AO should request specific security mitigations.